

## INDICE SOMMARIO

|   |       |
|---|-------|
| <b>Prefazione alla prima edizione</b> di <i>Antonello Soro</i> - Presidente del Garante per la protezione dei dati personali . . . . .                | XIII  |
| <b>Prefazione alla seconda edizione</b> di <i>Ginevra Cerrina Feroni</i> - Vice Presidente del Garante per la protezione dei dati personali . . . . . | XVII  |
| <i>Gli Autori</i> . . . . .   | XXIII |

### CAPITOLO 1

#### LA NORMATIVA DI RIFERIMENTO

di *Michele Iaselli*

|  |    |
|--|----|
| 1. Il concetto di privacy . . . . .  | 1  |
| 2. La normativa nazionale ed europea previgente il GDPR . . . . .  | 4  |
| 3. Il Regolamento Europeo . . . . .  | 9  |
| 4. La disciplina di adeguamento nazionale (d.lgs. 101/2018) e la riforma operata dal d.l. 139/2021 . . . . . | 24 |

### CAPITOLO 2

#### IL SISTEMA DI GESTIONE DELLA PRIVACY

di *Andrea d'Agostino*

|  |    |
|--|----|
| 1. Introduzione e contesto normativo . . . . .   | 35 |
| 2. La gestione dei dati personali: da una normativa prescrittiva alla responsabilizzazione delle imprese . . . . . | 37 |
| 3. L'evoluzione del sistema di gestione della privacy . . . . .  | 41 |
| 4. Conclusioni . . . . .   | 45 |

### CAPITOLO 3

#### I SOGGETTI PRIVACY

di *Gianluigi Marino*

|  |    |
|--|----|
| 1. I soggetti previsti dal GDPR . . . . .  | 47 |
| 2. Il titolare del trattamento . . . . .   | 49 |
| 3. I contitolari . . . . .   | 54 |
| 4. Il responsabile del trattamento (e i sub-responsabili) . . . . .              | 58 |
| 5. Rappresentanti di titolare e responsabile non stabiliti nell'Unione . . . . . | 64 |

|    |   |    |
|----|---|----|
| 6. | <i>Data protection officer</i> (rinvio) . . . . . | 66 |
| 7. | Interessato . . . . .                             | 66 |

## CAPITOLO 4

**I DIRITTI DEGLI INTERESSATI**di *Gianluigi Marino*

|     |   |     |
|-----|---|-----|
| 1.  | Premessa . . . . .  | 73  |
| 2.  | Tempi, modalità e costi dell'esercizio dei diritti da parte dell'interessato . . . . .  | 74  |
| 3.  | Le limitazioni dei diritti previste dal GDPR e dal diritto italiano. I diritti riguardanti le persone decedute . . . . .                | 76  |
| 4.  | Il diritto ad essere informati . . . . .  | 80  |
| 5.  | Il diritto di accesso dell'interessato . . . . .  | 87  |
| 6.  | Il diritto di rettifica . . . . .   | 90  |
| 7.  | Il diritto alla cancellazione . . . . .   | 92  |
| 8.  | Il diritto di limitazione del trattamento . . . . .   | 97  |
| 9.  | Il diritto alla portabilità dei dati . . . . .  | 98  |
| 10. | Il diritto di opposizione . . . . .   | 102 |
| 11. | Il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione . . . . . | 104 |
| 12. | Sanzioni . . . . .  | 107 |

## CAPITOLO 5

**IL CONSENSO COME CONDIZIONE DI LICEITÀ**di *Lucio Scudiero*

|     |  |     |
|-----|--|-----|
| 1.  | Il consenso dell'interessato nel più generale tema della liceità del trattamento . . . . . | 109 |
| 2.  | La validità del consenso: i requisiti del consenso nel GDPR . . . . .                      | 110 |
| 3.  | ( <i>Segue</i> ): il consenso informato . . . . .  | 111 |
| 4.  | ( <i>Segue</i> ): il consenso libero . . . . .   | 115 |
|     | 4.1. ( <i>Segue</i> ): squilibrio di potere . . . . .                                      | 116 |
|     | 4.2. ( <i>Segue</i> ): condizionalità . . . . .  | 117 |
|     | 4.3. ( <i>Segue</i> ): vantaggio e pregiudizio . . . . .                                   | 121 |
| 5.  | ( <i>Segue</i> ): il consenso specifico . . . . .  | 122 |
| 6.  | ( <i>Segue</i> ): il consenso inequivocabile . . . . .                                     | 125 |
| 7.  | ( <i>Segue</i> ): il consenso dimostrabile . . . . .                                       | 126 |
| 8.  | ( <i>Segue</i> ): il consenso revocabile . . . . .   | 130 |
| 9.  | ( <i>Segue</i> ): il consenso espresso o esplicito . . . . .                               | 133 |
| 10. | Il consenso dei minori . . . . .   | 134 |
| 11. | Conclusioni . . . . .  | 135 |

## CAPITOLO 6

**IL REGISTRO DEI TRATTAMENTI**di *Roberta Quintavalle*

|    |                                       |     |
|----|---------------------------------------|-----|
| 1. | La normativa di riferimento . . . . . | 137 |
| 2. | Cosa deve fare il titolare . . . . .  | 138 |

|    |   |     |
|----|---|-----|
| 3. | Cosa deve fare il responsabile . . . . .  | 139 |
| 4. | Chi ha l'obbligo di tenuta del Registro delle attività di trattamento . . . . . | 140 |
| 5. | L'impatto in azienda e le funzioni coinvolte . . . . .                          | 142 |
| 6. | Come predisporre il Registro . . . . .  | 143 |
| 7. | La <i>check list</i> per il Registro . . . . .                                  | 145 |
| 8. | Come gestire il Registro . . . . .  | 147 |

## CAPITOLO 7

**LA PROFILAZIONE**di *Iacopo Destri e Anna Maria Lotto*

|      |  |     |
|------|--|-----|
| 1.   | Introduzione . . . . .   | 151 |
| 2.   | Definizione e quadro normativo . . . . .   | 152 |
| 3.   | Disciplina sulla profilazione . . . . .  | 154 |
| 3.1. | Previsioni generali applicabili in materia di profilazione e di processi decisionali automatizzati . . . . . | 156 |
| 3.2. | Processi decisionali esclusivamente automatizzati, compresa la profilazione . . . . .                        | 161 |
| 3.3. | Valutazione di impatto e responsabile della protezione dei dati . . . . .                                    | 165 |
| 3.4. | Profilazione e minori . . . . .  | 165 |
| 3.5. | Profilazione avente ad oggetto dati raccolti <i>online</i> e disciplina di dettaglio applicabile. . . . .    | 167 |
| 4.   | Riflessioni conclusive . . . . .   | 171 |

## CAPITOLO 8

**SICUREZZA DEI DATI E VALUTAZIONE DEI RISCHI**di *Ulrico Bardari*

|        |  |     |
|--------|--|-----|
| 1.     | Introduzione: dalla privacy alla sicurezza . . . . .   | 177 |
| 2.     | Valutazione dell'impatto sulla privacy . . . . .   | 179 |
| 2.1.   | Metodologie, standard e linee guida GDPR . . . . .   | 180 |
| 2.2.   | Comprendere le differenze tra PIA e DPIA del GDPR . . . . .  | 181 |
| 2.3.   | Il panorama attuale nei quadri e strumenti PIA . . . . .   | 183 |
| 3.     | Valutazione dei rischi . . . . .   | 187 |
| 3.1.   | Flussi di elaborazione dei dati nel quadro del GDPR . . . . .  | 187 |
| 3.2.   | Sistema di punteggio dell'impatto sulla privacy . . . . .  | 187 |
| 3.3.   | Caratterizzazione delle vulnerabilità . . . . .  | 189 |
| 3.4.   | Impatto sulla privacy . . . . .  | 190 |
| 3.4.1. | Livello di impatto . . . . .   | 190 |
| 3.4.2. | Ambito dell'impatto . . . . .  | 193 |
| 3.4.3. | Tipi di dati . . . . .   | 193 |
| 3.5.   | Punteggi sulla privacy delle attività di trattamento . . . . .   | 194 |
| 4.     | Valutazione dei rischi per la sicurezza informatica e la privacy: la strada da percorrere . . . . .            | 196 |
| 4.1.   | Valutazione dei rischi per la sicurezza informatica e la privacy per le catene di approvvigionamento . . . . . | 196 |
| 4.2.   | Connessione tra mondo fisico e mondo cibernetico . . . . .   | 197 |
| 4.3.   | Mitigazione del rischio attraverso la selezione ottimale delle contromisure . . . . .                          | 197 |
| 5.     | Conclusioni . . . . .  | 199 |

## CAPITOLO 9

**IL DATA PROTECTION OFFICER**di *Giovanni Battista Gallus e Michela Pintus*

|       |  |     |
|-------|--|-----|
| 1.    | Introduzione . . . . .   | 201 |
| 2.    | Il DPO nel GDPR . . . . .  | 203 |
| 2.1.  | L'obbligatorietà della nomina: enti e organismi pubblici. . . . .  | 203 |
| 2.2.  | L'obbligatorietà della nomina: enti privati. . . . .   | 206 |
| 2.3.  | La nomina facoltativa. . . . .   | 211 |
| 2.4.  | La nomina del DPO. . . . .   | 211 |
| 2.5.  | La nomina del DPO nel settore pubblico. . . . .  | 213 |
| 2.6.  | La nomina del DPO nel settore privato. . . . .   | 217 |
| 2.7.  | La competenza specialistica e la capacità di assolvere i compiti come cardine nell'individuazione del DPO. . . . . | 218 |
| 2.8.  | La posizione del DPO nelle organizzazioni pubbliche e private. . . . .   | 220 |
| 2.9.  | La pubblicità dei dati di contatto del DPO e le sue interazioni con gli interessati. . . . .                       | 221 |
| 2.10. | Compiti e responsabilità del DPO . . . . .   | 223 |

## CAPITOLO 10

**DATA PROTECTION IMPACT ASSESSMENT**di *Giovanni Battista Gallus e Michela Pintus*

|    |   |     |
|----|---|-----|
| 1. | Introduzione . . . . .  | 227 |
| 2. | Definizione e presupposti . . . . .   | 229 |
| 3. | Le ipotesi specifiche individuate dal GDPR . . . . .                        | 234 |
| 4. | Il procedimento di valutazione di impatto e la sua documentazione . . . . . | 236 |
| 5. | La consultazione preventiva . . . . .                                       | 240 |
| 6. | La disciplina transitoria e la novella del d.l. 139/2021 . . . . .          | 242 |

## CAPITOLO 11

**LA NOTIFICAZIONE E LA COMUNICAZIONE DI UNA VIOLAZIONE DEI DATI PERSONALI (“DATA BREACH”)**di *Giovanni Battista Gallus*

|      |  |     |
|------|--|-----|
| 1.   | Introduzione . . . . .   | 245 |
| 2.   | La definizione di “violazione dei dati personali” . . . . .                                | 248 |
| 3.   | La notificazione al Garante . . . . .  | 251 |
| 3.1. | Il termine per la notificazione . . . . .  | 253 |
| 3.2. | Il ruolo del <i>data processor</i> . . . . .   | 254 |
| 3.3. | Modalità della notificazione . . . . .   | 255 |
| 4.   | La comunicazione agli interessati . . . . .  | 258 |
| 4.1. | Il contenuto e le modalità della comunicazione agli interessati . . . . .                  | 259 |
| 4.2. | Le ipotesi di esclusione dell'obbligo di comunicazione agli interessati . . . . .          | 261 |
| 5.   | La formalizzazione e documentazione delle attività inerenti i <i>data breach</i> . . . . . | 263 |
| 6.   | Il ruolo del DPO nella gestione dei <i>data breach</i> . . . . .                           | 265 |
| 7.   | I rapporti con altre tipologie di <i>data breach</i> . . . . .                             | 266 |

## CAPITOLO 12

**IL TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI  
O ORGANIZZAZIONI INTERNAZIONALI**di *Vincenzo Colarocco*

|        |   |     |
|--------|---|-----|
| 1.     | La normativa di riferimento . . . . .   | 269 |
| 2.     | Il Garante per la protezione dei dati personali, il Gruppo di lavoro <i>ex</i><br>Articolo 29 . . . . .                             | 272 |
| 3.     | Trasferimento di dati personali: l'esperienza del Codice . . . . .  | 274 |
| 4.     | Regolamento e trasferimento dei dati personali . . . . .  | 276 |
| 5.     | La decisione di adeguatezza . . . . .   | 278 |
| 5.1.   | Elenco Paesi autorizzati . . . . .  | 280 |
| 5.2.   | Trasferimento dati in USA: <i>Safe Harbor</i> , <i>Privacy Shield</i> e le<br>sentenze <i>Schrems</i> e <i>Schrems II</i> . . . . . | 281 |
| 6.     | Trasferimento soggetto a garanzie adeguate . . . . .  | 284 |
| 6.1.   | Norme vincolanti d'impresa. . . . .   | 286 |
| 6.2.   | Clausole contrattuali standard. . . . .   | 291 |
| 6.2.1. | L'applicazione delle SCC: i provvedimenti dell'Auto-<br>rità austriaca e dell'EDPS nel caso <i>Google Analytics</i> .               | 293 |
| 7.     | Trasferimenti vietati . . . . .   | 297 |
| 8.     | Deroghe . . . . .   | 297 |
| 9.     | Conclusioni . . . . .   | 300 |

## CAPITOLO 13

**BIG DATA E INTERNET OF THINGS:  
DATA PROTECTION E DATA GOVERNANCE  
ALLA LUCE DEL REGOLAMENTO EUROPEO**di *Fernanda Faini*

|      |   |     |
|------|---|-----|
| 1.   | <i>Big data</i> e <i>Internet of Things</i> . . . . .   | 303 |
| 2.   | Il diritto incontra i "grandi dati": profili giuridici e implicazioni so-<br>ciali . . . . .                        | 307 |
| 3.   | La <i>data protection</i> nei <i>big data</i> e nell' <i>Internet of Things</i> . . . . .                           | 311 |
| 3.1. | Principi e strumenti del Regolamento UE 2016/679 da impie-<br>gare e valorizzare nell'era degli algoritmi . . . . . | 313 |
| 3.2. | Aspetti problematici . . . . .  | 316 |
| 4.   | Possibili soluzioni e suggestioni future . . . . .  | 319 |

## CAPITOLO 14

**INTELLIGENZA ARTIFICIALE E ROBOTICA**di *Michele Iaselli*

|      |  |     |
|------|--|-----|
| 1.   | Cos'è la robotica . . . . .                                | 327 |
| 2.   | Le applicazioni della robotica . . . . .                   | 329 |
| 3.   | Il problema della regolamentazione giuridica . . . . .     | 333 |
| 3.1. | Etica e responsabilità . . . . .                           | 335 |
| 3.2. | Privacy e sicurezza . . . . .                              | 339 |
| 4.   | L'intelligenza artificiale . . . . .                       | 341 |
| 4.1. | I risvolti etici dell'IA . . . . .                         | 356 |
| 4.2. | La proposta di Regolamento della Commissione Europea . . . | 361 |
| 5.   | Conclusioni . . . . .                                      | 366 |

## CAPITOLO 15

**TRATTAMENTO DI DATI PERSONALI  
PER SCOPI DI RICERCA SCIENTIFICA**di *Stefania Stefanelli*

|    |  |     |
|----|--|-----|
| 1. | Dati identificativi diretti ed indiretti/identificazione e identificabilità . . . . .              | 369 |
| 2. | Condizioni di liceità del trattamento a fini di ricerca scientifica . . . . .                      | 372 |
| 3. | Principio di limitazione delle finalità . . . . .  | 376 |
| 4. | Espressione del consenso alla sperimentazione e al trattamento dei dati . . . . .                  | 378 |
| 5. | Diritto all'autodeterminazione e partecipazione di minori e incapaci alla ricerca . . . . .        | 383 |
| 6. | Trattamento dei dati personali in assenza di consenso . . . . .                                    | 387 |
| 7. | Durata del trattamento e trattamento ulteriore . . . . .   | 392 |
| 8. | Comunicazione e diritti degli interessati: efficacia generale delle regole deontologiche . . . . . | 396 |

## CAPITOLO 16

**LA CERTIFICAZIONE DEI CONSENSI RACCOLTI ONLINE**di *Tommaso Grotto e Emanuele Casadio*

|     |  |     |
|-----|--|-----|
| 1.  | I dati come <i>asset</i> strategico alla luce dei <i>big data</i> e del GDPR . . . . .   | 399 |
| 2.  | Il ciclo di vita dei consensi . . . . .  | 400 |
| 3.  | La verificabilità dei consensi . . . . .   | 400 |
| 4.  | Il regime sanzionatorio . . . . .  | 401 |
| 5.  | Il ciclo di vita dei dati personali analogici e digitali . . . . .   | 401 |
| 6.  | Il valore probatorio delle firme elettroniche semplici, avanzate e qualificate . . . . .   | 403 |
| 7.  | L'acquisizione di un dato informatico secondo lo standard ISO/IEC 27037:2012 . . . . .   | 406 |
| 8.  | L'acquisizione forense e la gestione dei consensi . . . . .  | 409 |
| 9.  | Le <i>Consent Management Platform</i> ed il <i>framework</i> di <i>IAB Europe</i> . . . . .  | 413 |
| 10. | Il valore probatorio dei consensi acquisiti secondo lo standard ISO/IEC 27037:2012 e i precedenti giurisprudenziali a supporto . . . . . | 414 |
| 11. | I vantaggi collegati alla certificazione dei consensi . . . . .  | 415 |

## CAPITOLO 17

**LA RESPONSABILITÀ CIVILE E  
DANNO DA TRATTAMENTO ILLECITO  
DEI DATI ALLA LUCE DEL REGOLAMENTO UE 2016/679**di *Michela Barbarossa, Chiara Benvenuto e Valeria Cerocchi*

|      |  |     |
|------|--|-----|
| 1.   | Il diritto al risarcimento del danno da trattamento illecito di dati personali: evoluzione . . . . .                   | 417 |
| 2.   | L'art. 82 del GDPR: le scelte del legislatore europeo . . . . .  | 418 |
| 2.1. | Il danno risarcibile . . . . .   | 422 |
| 2.2. | I soggetti responsabili: la responsabilità solidale. . . . .   | 423 |
| 2.3. | La prova liberatoria alla luce del principio di <i>accountability</i> . . . . .  | 428 |
| 2.4. | Il decreto legislativo attuativo . . . . .   | 430 |
| 3.   | La tutela giurisdizionale ed il ruolo dell'autorità di controllo: la questione della competenza territoriale . . . . . | 431 |

|    |   |     |
|----|---|-----|
| 4. | L'orientamento francese . . . . .   | 434 |
| 5. | L'ipotesi di trattamento illecito alla luce delle novità introdotte dal Regolamento . . . . . | 434 |
| 6. | Conclusioni . . . . .   | 440 |

## CAPITOLO 18

**SANZIONI E RESPONSABILITÀ AMMINISTRATIVE E PENALI**di *Francesco Paolo Micozzi*

|      |  |     |
|------|--|-----|
| 1.   | Introduzione . . . . .   | 443 |
| 2.   | Le misure di cui all'art. 58 rilevanti in ambito sanzionatorio . . . . .   | 446 |
| 3.   | Le sanzioni amministrative . . . . .   | 449 |
| 4.   | Le ipotesi di sanzioni amministrative pecuniarie previste dal GDPR . . . . .   | 450 |
| 4.1. | Le sanzioni amministrative pecuniarie del quarto comma dell'art. 83 del GDPR . . . . .   | 452 |
| 4.2. | Le sanzioni amministrative pecuniarie del quinto comma dell'art. 83 del GDPR . . . . .   | 457 |
| 5.   | Elementi per la individuazione e quantificazione della sanzione amministrativa pecuniaria . . . . .  | 458 |
| 6.   | Criteri applicativi e procedimento sanzionatorio e correttivo secondo il decreto legislativo di armonizzazione . . . . .                       | 463 |
| 7.   | Le altre sanzioni amministrative o penali . . . . .  | 474 |
| 8.   | Il trattamento illecito di dati (art. 167) . . . . .   | 476 |
| 9.   | Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala (art. 167-bis) . . . . .                           | 481 |
| 10.  | Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala (art. 167-ter) . . . . .                                      | 483 |
| 11.  | Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante (art. 168) . . . . . | 483 |
| 12.  | Inosservanza di provvedimenti del Garante (art. 170) . . . . .   | 484 |
| 13.  | Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori (art. 171) . . . . .                 | 485 |
| 14.  | Questioni ulteriori . . . . .  | 486 |
| 15.  | Le norme penali incriminatrici del d.lgs. 51/2018 . . . . .  | 488 |
| 16.  | <i>Ne bis in idem</i> . . . . .  | 491 |
| 17.  | Disposizioni transitorie e finali . . . . .  | 496 |

